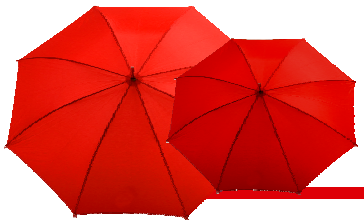
HowTo

Avira AntiVir WebGate (Suite)

Settings and Configuration

Avira Support

October 2009



Content

1 Which environment can be protected by Avira AntiVir WebGate? *2*

2 Installation *2*

3 Recommended Basic Configuration *3*

4 What can be configured additionally? *4*

4.1 Proxy settings **4**

4.2 Activation of an ICAP Server **4**

4.3 Activation of an HTTPS Tunnel **4**

4.4 Progress bar **5**

4.5 X-Header **5**

4.6 Clients authorized to access **5**

5 Particularities *6*

5.1 Squid as proxy server **6**

5.2 ICAP configuration **6**

6 Update Configuration *7*

6.1 Reasonable values for an update **7**

6.2 Large Enterprises **7**

6.3 Small Business **7**

6.4 Customers with narrow strip connections (Modem/ISDN): **8**

6.5 Internet Service Providers **8**

7 WebGate Suite Features *9*

1 Which environment can be protected by Avira AntiVir WebGate?

- Avira AntiVir WebGate can be used as proxy server with HTTP or FTP via HTTP supervision

- Avira AntiVir WebGate can work in front of or behind a further proxy server

- It can be used as an integration into an ICAP (Internet Content Adaptation Protocol) environment

- It works as an access control on the basis of the client's IP address or the target port

2 Installation

- Decompress: gzip -d antivir-webgate-prof.tgz

- Unpack: tar -xvf antivir-webgate-prof.tgz

- Change directory: cd antivir-webgate-prof.tgz

- Execute installation: ./install

Follow the installation dialogue ...

The following requests are recommended and should be kept

- Would you like to setup Engine and Signature updates as cron task ? [y]

- Please specify the interval to check. Recommended values are daily or 2 hours. available options: d [2]

- Please specify if boot scripts should be set up.
Set up boot scripts [y]

3 Recommended Basic Configuration

HTTP Port
HTTPPort 8080
Due to this command WebGate listens on port 8080. In case the port is already occupied by another proxy server service the port has to be changed accordingly.

FTP Port
FTPPort 2121
WebGate offers an FTP proxy service. In case the port is already occupied by another proxy server service the port has to be changed accordingly.

Quarantine directory
MoveConcerningFilesTo /home/quarantine
In case of a detection the file is moved into the quarantine directory and renamed. Therefore the file cannot be opened anymore by the user. But the file is not deleted or changed because false positives are possible.

Defining log files
LogFile /var/log/avwebgate.log
The command defines the log file of the OnAccess Scanner. It writes into the syslog by default.

Defining the quality of the information
LogLevel 4
This command defines a medium log level. It records alerts (e.g. detections), error messages (e.g. incorrect ACL configurations) and warnings (e.g. in case of encrypted archives).

Activates the heuristics on the medium level
HeuristicsLevel 2
A good balance between detection and early detection which prevents a lot of possible false positives.

Activates the detection of possible macro viruses in office documents
HeuristicsMacro yes
We recommend you the scan of office documents for an optimum of security.

4 What can be configured additionally?

These settings should be reconsidered before and only be used as and if required! The values have to be adjusted accordingly.

4.1 Proxy settings

The following proxy settings are necessary in order to integrate a corresponding proxy server in front of WebGate.

HTTPProxyServer your.proxy

HTTPProxyPort 3128

HTTPProxyUsername username

HTTPProxyPassword password

FTPProxyServer your.proxy

FTPProxyPort 2121

4.2 Activation of an ICAP Server

This activates the ICAP server of WebGate. The service runs additionally on the selected port. The ICAP server supports reqmod (Request modification) as well as respmod (Response modification).

Squid supports ICAP 1.0 with the version 3.x!
ICAPPort 1344

4.3 Activation of an HTTPS Tunnel

WebGate blocks the HTTPS data traffic by default as this traffic can’t be scanned due to its encryption.
If you want to tunnel the HTTPS sites, you can use the following parameter:
The HTTPS data traffic will NOT be scanned.

AllowHTTPSTunnel 1

4.4 Progress bar

Display of a site in the browser which shows a progress bar in case of huge downloads.
Additionally you have to define an interval in seconds (e.g. 3 seconds) which sends a refresh command to the browser.
The activation and configuration of the progress bar is proceeded by the following parameter:

RefreshInterval 3

4.5 X-Header

This command adds an X-header of the client to the request in order to inform a downstream proxy server about the requesting client.

AddXForwardedForHeader 1

4.6 Clients authorized to access

This command defines the clients authorized to access.
Unauthorized clients which want to access to WebGate are blocked.

AllowClientAddresses 127.0.0.1 192.168.0.0/16

5 Particularities

5.1 Squid as proxy server

This configuration sends all requests of the client to the squid via WebGate. So you can use the squid proxy functions.

Necessary settings in the squid.conf

cache_peer <WebGateHost> parent <WebGatePort> 0 no-query no-digest default

acl ALL src 0.0.0.0/0.0.0.0

never_direct allow ALL

5.2 ICAP configuration

By means of the start of the ICAP server which is described in chapter 4.2 the squid can work as ICAP client in order to handle requests.

Necessary settings in the squid.conf

icap_enable on

icap_service service_1 reqmod_precache 0 icap://[WEBGATE_HOST]:1344/reqmod

icap_service service_2 respmod_precache 0
icap://[WEBGATE_HOST]:1344/respmod

icap_class class_1 service_1

icap_class class_2 service_2

icap_access class_1 allow all

icap_access class_2 allow all

6 Update Configuration

In order to keep your AntiVir installation up-to-date you can configure two different modes of updates during the installation:

- Scanner update (only Scanner & Engine & VDF)
- Product update (Guard program files)

You find the settings for the updates in the following file after the installation:

/etc/cron.d/avira_updater:

00 */2 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
15 12 * * Tü root /usr/lib/AntiVir/avupdate --product=Guard

6.1 Reasonable values for an update

Depending on the target group we recommend our customers to proceed an update at least 2 or 3 times a day.

6.2 Large Enterprises

Example: hourly update

/etc/cron.d/avira_updater:

* */1 * * * root /usr/lib/AntiVir/avupdate --product=Scanner

6.3 Small Business

Example: 3 hour interval

/etc/cron.d/avira_updater:

* */3 * * * root /usr/lib/AntiVir/avupdate --product=Scanner

6.4 Customers with narrow strip connections (Modem/ISDN):

Example: 8 hour interval

/etc/cron.d/avira_updater:

* */8 * * * root /usr/lib/AntiVir/avupdate --product=Scanner

6.5 Internet Service Providers

It is recommended for internet service providers to download the current signatures more frequently, e.g. every 15 minutes. Thereby you can make sure to use always the latest signatures.

/etc/cron.d/avira_updater:

*/15 * * * * root /usr/lib/AntiVir/avupdate --product=Scanner

Furthermore you have the possibility to execute only an engine and VDF update. The guard product files and the central scanner service (SAVAPI) are not updated.

This can be interesting for you in case you are considering program updates as especially sensitive. Thereby you have the possibility to proceed an audit on a separate test system before you implement the new version in the productive network.

The command has to be entered as follows:

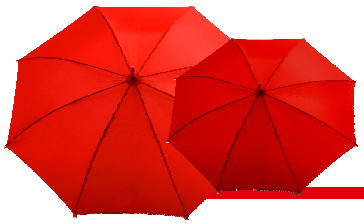
$ /usr/lib/AntiVir/avupdate --product=Signatures

7 WebGate Suite Features

The WebGate Suite Feature allows you to block certain categories of websites.
E.g. sites containing pornography, phishing, malware and fraud can be blocked.

Definition of filter categories:

Numeric Value	Category
0	Pornography
1	Erotic / Sex
2	Swimwear / Lingerie
3	Shopping
4	Auctions / Classified Ads
5	Governmental Organizations
6	Non-Governmental Organizations
7	Cities / Regions / Countries



8	Education
9	Political Parties
10	Religion
11	Sects
12	Illegal Activities
13	Computer Crime
14	Political Extreme / Hate / Discrimination
15	Warez / Hacking / Illegal Software
16	Violence / Extreme
17	Gambling / Lottery
18	Computer Games
19	Toys

| 20 | Cinema / Television |

| 21 | Recreational Facilities / Amusement / Theme Parks |

| 22 | Art / Museums / Memorials / Monuments |

| 23 | Music |

| 24 | Literature / Books |

| 25 | Humor / Comics |

| 26 | General News / Newspapers / Magazines |

| 27 | Web Mail |

| 28 | Chat |

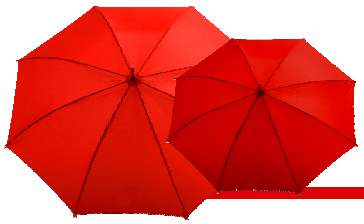
| 29 | Newsgroups / Bulletin Boards / Blogs |

| 30 | Mobile Telephony |

| 31 | Digital Postcards |

32	Search Engines / Web Catalogs / Portals
33	Software / Hardware / Distributors
34	Communication Services
35	IT Security / IT Information
36	Website Translation
37	Anonymous Proxies
38	Illegal Drugs
39	Alcohol
40	Tobacco
41	Self-Help / Addiction
42	Dating / Relationships
43	Restaurants / Bars

44	Travel
45	Fashion / Cosmetics / Jewelry
46	Sports
47	Building / Residence / Architecture / Furniture
48	Nature / Environment / Animals
49	Personal Homepages
50	Job Search
51	Investment Brokers / Stocks
52	Financial Services / Investment / Insurance
53	Banking / Home Banking
54	Vehicles / Transportation



| 55 | Weapons / Military |

| 56 | Health |

| 57 | Abortion |

| 59 | Spam URLs |

| 60 | Malware |

| 61 | Phishing URLs |

| 62 | Instant Messaging |

Parameter in the /etc/avwebgate.conf

Blocks websites of the categories Pornography (0) _BIS_ Swimwear / Lingerie (2) (contains Erotic / Sex [1])

and illegal Activities (12) _UND_ Political Extreme / Hate / Discrimination (14) _AND_ Phishing URLs (61)

WSBlockCategories 0-2 12 14 61

##

You find further information and setting possibilities of Avrira AntiVir WebGate (Suite) in the manual or in our knowledgebase on

http://www1.avira.com/en/support/kbsearch.php